Sub a2

WHAT IS CLAIMED IS:

1. A method for withdrawing an encryption key from a key escrow database, comprising:

creating a set of N trap door encryption-decryption function pairs each paired with a corresponding token;

transmitting the set of N trap door encryption-decryption function pairs to a receiver;

randomly selecting at the receiver one of the trap door encryption-decryption function pairs and the paired token;

adding randomization information to the selected trap door encryption-decryption function pair and the corresponding token;

encrypting a decryption key using the corresponding token with the randomly selected encryption-decryption function pair;

recording the created set of N trap door encryption-decryption function pairs and the corresponding paired token;

recording the encrypted randomly selected trap door encryption-decryption function pair along with the decryption key in a key escrow database; and

inverting the created set of N trap door encryption-decryption function pairs and the encrypted randomly selected trap door encryption-decryption function pair along with the decryption key to identify the decryption key.

2. A method for withdrawing an encryption key from a key escrow database as in Claim 1, further comprising:

encrypting the created set of N trap door, the encryption-decryption function pairs and the randomly

selected trap door function along with the decryption key prior to recording in an escrow database.

3. The method for withdrawing an encryption key from a key escrow database as in Claim 1, further comprising:

randomly selecting at the receiver an additional trap door encryption-decryption function pair and the paired token;

adding randomization information to the additional selected trap door encryption-decryption function pair and the corresponding token;

concatenating the results of the adding of randomization information to the additional selected trap door encryption-decryption function pair to the encryption of the randomly selected first trap door encryption-decryption function pair; and

encrypting the concatenating results using the encryption key from the second choice.

4. The method for withdrawing an encryption key from a key escrow database as in Claim 1 further comprising adding signature information to the selected trap door encryption-decryption function pair to distinguish valid subsequent decodings from invalid decodings.

5. The method for withdrawing an encryption key from a key escrow database as in Claim 1, wherein encrypting a selected trap door encryption-decryption function pair comprises calculating a cryptogram utilizing the corresponding token and including an encryption key along with randomization information, as

well as additional information added for signature purposes.

6. A method for withdrawing encryption keys from a key escrow database, comprising:

generating, in accordance with a selected encryption function, a set of *N* cryptogram/decryption key pairs, each pair having a corresponding token;

transmitting the set of N cryptogram/decryption key pairs to a receiver;

randomly selecting at the receiver one of the cryptogram/decryption key pairs along with the corresponding token;

decrypting the randomly selected cryptogram utilizing the corresponding token to obtain a corresponding encryption key;

generating a cryptogram utilizing the corresponding encryption key and comprising the selected token and randomization information;

recording in an escrow database the generated set of N cryptogram/decryption key pairs along with each corresponding token and the generated cryptogram based on the randomly selected cryptogram decryption key pair; and

inverting the recorded set of N cryptogram/decryption key pairs and the generated cryptogram to identify an encryption key from the key escrow database.

7. The method for withdrawing encryption keys from a key escrow database as in Claim 6, further comprising:

randomly selecting at the receiver one or more additional *N* cryptogram/decryption key pairs and corresponding tokens;

decrypting each cryptogram using the associated token of the additionally selected encryption/decryption

key pairs to identify a corresponding encryption key for each additionally selected pair;

generating a response cryptogram for each additionally selected cryptogram/decryption key pair utilizing the corresponding encryption key and comprising the selected token and randomization information; and

mixing the token information from one selected pair with the response cryptogram from a different selected pair along with randomization information to diffuse response structure prior to generating another response cryptogram.

8. The method for withdrawing encryption keys from a key escrow database as in Claim 6, further comprising:

decrypting the cryptogram of a cryptogram/decryption key pair using the associated decryption key to identify token information.

9. The method for withdrawing encryption keys from a key escrow database as in Claim 8 wherein mixing comprises utilization of a linear transform.

10. The method for withdrawing encryption keys from a key escrow database as in Claim 8 wherein mixing comprises utilization of a symmetrical cryptosystem.

11. The method for withdrawing encryption keys from a key escrow database as in Claim 8 wherein mixing further comprises utilization of a public key cryptosystem.

12. The method for withdrawing encryption keys from a key escrow database as in Claim 6 wherein recording in an escrow database further comprises encrypting the generated set of N cryptogram decryption key pairs and the response message prior to recording.

13. The method for withdrawing encryption keys from a key escrow database as in Claim 6 further comprising adding signature information to the response message to enable valid decodings to be distinguished from invalid decodings.

14. A method for secure communication between an originator and a receiver using message encryption, comprising:

creating at an originator a set of N trap door functions each paired with a corresponding token, each trap door function comprising a cryptogram/decryption key pair;

transmitting the set of N trap door functions to a receiver;

randomly selecting at the receiver one of the trap door functions and the paired token;

adding randomization information to the corresponding token of the selected trap door function;

encrypting an escrow key with the randomly selected trap door function;

transmitting the encrypted key with the randomly selected trap door function to the originator; and

decoding the encrypted escrow key with the randomly selected trap door function utilizing retained trap door information.

15. The process as in Claim 14 further comprising decrypting the cryptogram to identify the corresponding token utilizing the decryption key of the cryptogram/decryption key pair.

16. The method as in Claim 15 wherein encrypting an escrow key comprises generating a cryptogram comprising the corresponding token, the decryption key and randomization information.

17. The method of Claim 14 wherein decoding the encrypted key comprises selecting a decryption key randomly from a selected group of decryption keys.

18. The method of Claim 17 further comprising recognizing a correct decoding result utilizing structural information embedded in the response message.

19. The method of Claim 14 wherein creating at an originator further comprises generating the set of N trap door functions utilizing a selected encryption function and a private encryption key.

Add a3

Add B2